



IBM Software Group

Lessons in Secure Engineering

Andras R. Szakal

IBM DE, Director Software Architecture

IBM Federal SWG

aszakal@us.ibm.com



IBM Lab Development Philosophy

- **Globally Integrated Development Team**
 - ▶ Common architecture, tools and process
 - ▶ Lightweight governance
 - ▶ Distributed skill pools leveraged world-wide as well as in local engagements
- **Continuous focus on effectiveness and efficiency**
 - ▶ Culture of reuse facilitated through common components and architecture
 - ▶ Incremental development approach with continuous customer feedback
 - ▶ Strong ongoing focus on consumability and quality
- **Strong sustained improvement**
 - ▶ Faster delivery, faster feedback, faster deployment, faster renewal rate
 - ▶ Reduced base development expense



Best Practices for Distributed Development Success

Sound Dev Gov Principles

- Lightweight central governance mechanisms
- Development Steering Committee
- Architecture Board
- Culture of Sharing and Reuse
- Developer Web Site
- Centralized Development Services

Enable for Success

- Tools not Rules
- Community Source
- Shared Asset Repository
- Best Practices
- Common Components
- Clearing House for Dependency Management

Execute Agile/Lean for Productivity

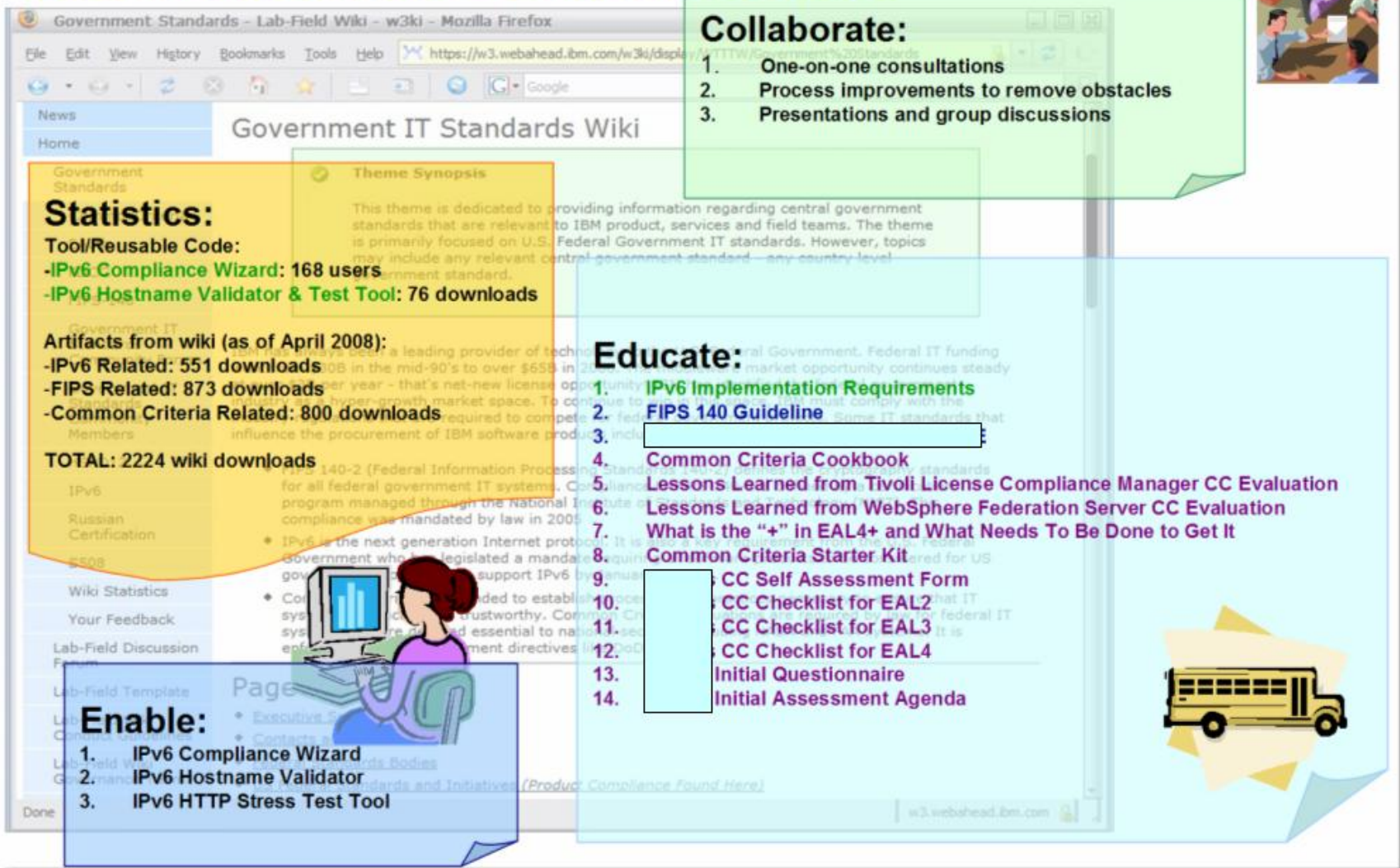
- Discipline, adaptive development approaches
- Continuous stakeholder feedback to understand changing needs
- Time-boxed iterations
- Eliminate waste, increase visibility

Guiding Principles for SW Dev

- SWG Architecture Blueprint
- Outside-in-Development
- Agile and Lean Approaches
- Modeling and Componentization
- Fostering Communities and Sharing Best Practices


Engineering Community - Leveraging Collaboration

Government Standards – Enablement Artifacts



Collaborate:

1. One-on-one consultations
2. Process improvements to remove obstacles
3. Presentations and group discussions



Statistics:

Tool/Reusable Code:

- IPv6 Compliance Wizard: 168 users
- IPv6 Hostname Validator & Test Tool: 76 downloads

Artifacts from wiki (as of April 2008):

- IPv6 Related: 551 downloads
- FIPS Related: 873 downloads
- Common Criteria Related: 800 downloads


TOTAL: 2224 wiki downloads

Enable:

1. IPv6 Compliance Wizard
2. IPv6 Hostname Validator
3. IPv6 HTTP Stress Test Tool

Educate:

1. IPv6 Implementation Requirements
2. FIPS 140 Guideline
3. [Redacted]
4. Common Criteria Cookbook
5. Lessons Learned from Tivoli License Compliance Manager CC Evaluation
6. Lessons Learned from WebSphere Federation Server CC Evaluation
7. What is the "+" in EAL4+ and What Needs To Be Done to Get It
8. Common Criteria Starter Kit
9. CC Self Assessment Form
10. CC Checklist for EAL2
11. CC Checklist for EAL3
12. CC Checklist for EAL4
13. Initial Questionnaire
14. Initial Assessment Agenda



Gov Stds community reuse / collaboration growing

Enable: increased reuse

	Oct 2007 (cumulative)	Oct 2008 (cumulative)	Increase Percentage
IPv6 Wizard usages	135	214	58%
IPv6 Reusable code download	48	68	42%

“... these resources save plenty of our time and provide a consistent source of all necessary information that individual development groups can use to achieve IPv6 enablement of their products “

Tivoli Network Management Development Team

Educate: increased wiki traffic and artifact download

	Oct 2007 (cumulative)	Oct 2008 (cumulative)	Increase Percentage
Wiki visitors	3680	9198	150 %
Artifact download	1547	3529	128 %

Collaborate:

- Resolve dependency issues to enable deliveries
- One-on-one consultations with product teams, resulting in mitigations of several revenue-impacting issues

Leveraging Web2.0 to Facilitate an SE Community



Secure Engineering Community

☐ Make this my preferred community
[Join the community](#)

Over the last few years, IBM and its customers have seen a disturbing rise in the number of successful attempts to leverage IT product vulnerabilities to obtain personal, corporate and government data by organized crime and even rogue member states. Recently, concerned customers have asked IBM for more details on how we ensure the quality and integrity of our software and hardware offerings; in particular, how IBM develops secure software/hardware -- how we ensure that our products are secure, or securable, and are unlikely to contain security vulnerabilities.

In addition, the U.S. federal government is considering policies which would limit the acquisition of IT products that do not meet certain assurance levels and use of secure coding standards by the vendor. In order to preserve our competitive advantage, we must continue to focus on these changing business dynamics and the resulting impact to our secure engineering practices.

The mission of the secure engineering community is to:

- View community information on the [Secure Engineering Community Wiki](#)
- Ask questions and provide answers in the [Secure Engineering Discussion Forum](#)
- View this [community](#) on the Lotus Community Server

Community bookmarks

- [Secure Engineering Wiki](#)
- [Secure Engineering Forum](#)

Community feeds

[Chris DeRobertis' Data Alchemy @ BlogCentral](#)

Wiki's
Forums
Feeds
Tagging
Asset Management

Subject Matter Experts

Expertise



[Andras Szakal](#)

[Click here for Bluecard](#) al SWG



[Christopher V Derobertis](#)

HPC Cluster Security Architect/Team Lead



[Timothy Hahn](#)

Distinguished Engineer, Chief Architect, Secure Systems and Networks



[Tony Nadalin](#)

Distinguished Engineer, Chief Security Architect



[Brian Snitzer](#)

Senior Technical Staff Member



[Nikola Vouk](#)

ITM Agent Developer (currently UNIX OS Agent)



[Jim Whitmore](#)

Senior Certified IT Architect

Welcome Andras Szakal | Log Out | Refresh RSS

SECURE ENGINEERING COMMUNITY [Home](#)

Search WCV2

Searching **seceng**

[Dashboard](#) > [Secure Engineering Community](#) > [Home](#)

Published on Apr 29, 2008

About Secure Engineering Community

IBM has long been considered a strong producer of high quality hardware and software. This reputation is well founded since many of our products are used in high performance, high stress, highly available environments which many of our customers view as mission critical to their businesses. Our customers and indeed many of our competitors look to us to lead the way in defining development practices and secure, based on the fact that we have been working within the computer industry for over 50 years.

Establishing an Agile Secure Engineering Community

- Teams need to collaborate across the development lifecycle
- Assurance practices are dynamic and change frequently
- Framework Based
- Automated



IBM's Secure Engineering Framework

- Enabled Through a Secure Engineering Framework
 - ▶ Decision Support Matrix
 - ▶ Best Practices
- Defines assurance activities by phase by product type
 - ▶ Set of deliverables / artifacts appropriate for the product profile (architecture)
- Establishes Risk Management Framework for Secure Engineering
 - ▶ Identify implications of decisions
 - ▶ Establishes mechanism for Risk Management / Mitigation



Secure Engineering Community - Leveraging Collaboration

- Development Automation is Key to Developer Adoption
 - ▶ Low ceremony = High Rate of Adoption
- Framework must be tools based
- Tooling must facilitate the development of the community
 - ▶ Collaborative team focused
 - ▶ Leverage Web2.0 Tooling
 - ▶ Integrate Education Services



धन्यवाद

Hindi

多謝

Traditional Chinese

ขอบคุณ

Thai

Спасибо

Russian

Gracias

Spanish

شكراً

Arabic

Thank You

Obrigado

Brazilian Portuguese

Grazie

Italian

Danke

German

Merci

French

நன்றி

Tamil

多谢

Simplified Chinese

감사합니다

Korean

ありがとうございました

Japanese

